CLAIMS

What is claimed is:

1. A method for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the multicast group in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, the method comprising the steps of:

creating and storing a group session key associated with the multicast group in a directory;

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory;

receiving a plurality of private keys from the subset of nodes;

receiving a new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the group session key through periodic replication of the directory;

communicating the new group session key private key to the first multicast proxy service node;

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys.

2. A method as recited in Claim 1, wherein authenticating the plurality of multicast proxy service nodes includes authenticating the plurality of multicast proxy service nodes based on a directory that comprises a directory system agent (DSA) that communicates with one or more of the multicast proxy service nodes and a replication service agent (RSA) that replicates attribute information of the one or more multicast proxy service nodes.

3. A method as recited in Claim 1, wherein receiving a new group session key includes receiving the new group session key from a node of a directory that comprises a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and a replication service agent (RSA) for replicating key information of the one or more multicast proxy service nodes.

4. A method as recited in Claim 3, further comprising the step of signaling the replication service agent to carry out replication by storing an updated group session key in a local node of the directory.

5. A method as recited in Claim 1, further comprising distributing a group session key to all nodes by creating and storing the group session key using a first multicast proxy service node of one domain of the directory; replicating the directory; and obtaining the group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

6. A method as recited in Claim 1, further comprising distributing a group session key to all nodes by creating and storing the group session key using a first multicast proxy service node of one domain of the directory; replicating the directory; and obtaining the group session key from a local multicast proxy service node that is a replica of the first multicast proxy service node.

7. A communication system for managing addition of a first multicast proxy service node to a secure multicast group that includes a plurality of other multicast proxy service nodes in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, the communication system comprising:

a group controller that creates and manages secure multicast communication among the other multicast proxy service nodes, having a private key;

a computer-readable medium comprising one or more instructions which, when executed by one or more processors, cause the one or more processors to carry out the steps of:

creating and storing a group session key associated with the multicast group in a directory;

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the multicast proxy service node to the multicast group, based on the group session key stored in the directory;

receiving a plurality of private keys from the subset of nodes;

receiving a new group session key for the multicast group, for use after addition of the first multicast proxy service node, from a local multicast proxy service node that has received the group session key through periodic replication of the directory;

communicating the new group session key private key to the first multicast proxy event service node;

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys.

8. A method for creating a secure multicast or broadcast group among a plurality of multicast proxy event service nodes, the method comprising the steps of:

authenticating the plurality of multicast proxy service nodes via a directory that includes a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes and for replicating attribute information of the one or more multicast proxy service nodes;

generating private keys for each of the multicast proxy service nodes, the private keys providing unique identification within the tree structure;

generating a first group session key for establishing the secure multicast or broadcast group among the multicast proxy service nodes;

distributing the first group session key among the multicast proxy service nodes by using periodic directory replication of the attribute information, wherein the attribute information comprises the first group session key, and the private keys; and

forming a second secure multicast group among the plurality of client nodes by one of the leaf nodes using a second group session key obtained

from a local replica of the node that generated the first group session key.

9. The method as recited in Claim 8, further comprising selectively updating the first group session key and the private keys using the DSA, wherein the step of selectively updating comprises:

detecting whether one of the nodes is leaving the secure multicast or broadcast group;

determining which of other nodes are affected by deletion of the leaving node;

updating the private keys of the affected intermediate nodes;

generating a new group session key;

modifying the attribute information based upon the updated private keys and the new group session key; and

distributing the modified attribute information using directory replication.

10. The method as recited in Claim 8, further comprising selectively updating the first group session key and the private keys via the DSA, wherein the step of selectively updating comprises:

receiving a request message from a new node to join the secure multicast or broadcast group;

determining which other nodes are affected by addition of the joining node;

updating the private keys of the affected nodes;

generating a new group session key and a private key of the new node;

modifying the attribute information based upon the updated private keys, the new group session key, and the private key of the new node; and

distributing the modified attribute information using directory replication.

11. A communication system for creating a secure multicast or broadcast group, the communication system comprising:

a plurality of multicast proxy service nodes, each of the multicast proxy service nodes having attribute information comprising a group identification value for uniquely identifying a particular one of the multicast proxy service nodes, wherein the plurality of multicast proxy service nodes form a logical arrangement of the multicast proxy service nodes according to a tree structure, the tree structure having a root node, intermediate nodes, and leaf nodes, one of the multicast proxy service node being designated as a primary multicast proxy service node, the primary multicast proxy service node being mapped to the root node, the other multicast proxy service nodes having private keys corresponding to the group identification values and being mapped to the intermediate nodes and the leaf nodes;

a directory comprising a directory system agent (DSA) for communicating with one or more of the multicast proxy service nodes to authenticate each of the multicast proxy service nodes and for replicating the attribute information of the one or more multicast proxy service nodes; and

a plurality of client nodes coupled to one of the multicast proxy service nodes, the one multicast proxy service node creating a secure multicast or broadcast client group that is separate from the secure multicast or broadcast group;

wherein one of the multicast proxy service nodes generates a first group session key for establishing the secure multicast or broadcast group

among the plurality of multicast proxy service nodes and distributes the first group session key to other nodes in the group using directory replication.

12. A computer system for establishing a secure multicast or broadcast group, the computer system comprising:

a communication interface for communicating with a plurality of external computer systems and for interfacing a directory to authenticate the computer system and the plurality of external computer systems;

a bus coupled to the communication interface for transferring data;

one or more processors coupled to the bus for selectively generating a group session key and private keys corresponding to the plurality of external computer systems, and for logically operating with the plurality of external computer systems according to a tree structure, the tree structure having a root node, intermediate nodes, and leaf nodes, wherein the computer system is mapped to the root node, the plurality of external computer systems are mapped to the intermediate nodes and the leaf nodes, the corresponding private keys providing unique identification of respective plurality of external computer systems within the tree structure, the group session key being distributed using directory replication using a directory system agent of the directory; and

a memory coupled to the one or more processors via the bus, the memory includes one or more sequences of instructions which when executed by the one or more processors cause the one or more processors to perform the step of selectively updating the group session key and the

private keys in response to whether a new client joins or a one of the client nodes leaves the multicast or broadcast group.

13. A computer-readable medium carrying one or more sequences of instructions for communicating a session key from a first multicast proxy service node of a secure multicast group to a plurality of other multicast proxy service nodes of the multicast group in a communication network, wherein each of the multicast proxy service nodes is capable of establishing multicast communication and serving as a key distribution center, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

creating and storing a group session key associated with the multicast group in a directory;

authenticating the first multicast proxy service node with a subset of the multicast proxy service nodes that are affected by an addition of the first multicast proxy service node to the multicast group, based on the group session key stored in the directory;

receiving a plurality of private keys from the subset of nodes;

receiving a new group session key for the multicast group for use after addition of the first multicast proxy service node from a local multicast proxy service node that has received the group session key through periodic replication of the directory;

communicating the new group session key private key to the first multicast proxy service node;

communicating a message to the subset of nodes that causes the subset of nodes to update their private keys.